PBMA Enhanced Security Work Groups

New User Authentication And Activation Plan (NUAAP)

Prepared for the

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Report No. 0190602.12.004

Revision 4.3

ARES CORPORATION
22800 Cedar Point Road
Cleveland, OH 44142

TABLE OF CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

1.1 Purpose

The Process Based Mission Assurance (PBMA) Enhanced Security Work Groups (ESWG) application is designed to provide users with secure collaborative Work Groups using a validated method of strong user authentication. The PBMA ESWG application enables the sharing of ACI data. This is information deemed as sensitive/critical data such as Source Evaluation Board (SEB) data, and information governed under the International Traffic Arms Regulated (ITAR) or Export Administration Regulations (EAR) laws.

The PBMA ESWG application operates behind the NASA Glenn Research Center (GRC) firewall. The Work Groups are designed to organize information, manage documents, share schedules and facilitate efficient project team collaboration, all in a browser-based environment. This fosters the exchange of information in an efficient, user-friendly manner.

The purpose of this document is to explain the roles and process involved in obtaining an Enhanced Security Work Group. Except for a brief explanation of the Work Group security settings in Security Practices, the application that runs the Work Groups is not discussed in this document. Information on the application functionality can be found in the PBMA Enhanced Security Administration Guide.

1.2 Roles

1.2.1 PBMA Enhanced Security Work Group Originator

The Work Group Originator ("Originator") makes the initial request for a new Work Group. The Originator is the data owner and assumes responsibility for all data that will reside in the Work Group.

⇒ See Process For Activating A New Work Group (Section 3) and Appendix B – National Agency Check Verification (Appendix B)for more information on the required paperwork to start an ACI-eligible Work Group.

If the Originator leaves and is no longer associated with the Work Group, a new Originator must fill the role. The required paperwork must be turned into PBMA Technical Support and signed by the current Originator whenever the role is handed to a new person.

1.2.2 PBMA Enhanced Security Work Group End-users

Work Group End-users ("End-users") refer to all users of the system. End-users are to read the PBMA ESWG Charter and uphold all security practices in Security Practices of this document.

1.2.3 PBMA Enhanced Security Work Group Technical Support

Work Group Technical Support ("Technical Support") is comprised of PBMA Information Technology (IT) personnel who are responsible for maintaining the backbone of the PBMA network, the Web site application, and the Help Desk. The Help Desk is the primary interface between the IT personnel and the Work Group end-users. Technical Support may also include other application support personnel when needed.

2 SECURITY PRACTICES

All new PBMA Work Groups are "secure work groups" because the servers in which they reside operate behind the NASA Glenn Research Center firewall and all traffic to and from the system is 128-bit encrypted. There are two types of requests for Work Groups; those Work Groups that will house ACI sensitive data and those that won't - requests will be made according to the one that best suits the Originator's needs.

All Work Group Originators, end-users and Technical Support personnel must take responsibility for protecting Administratively Controlled Information (ACI). ACI data must be safeguarded by protecting login information, properly configuring the Work Group, monitoring membership of the Work Group and information stored in a Work Group.

2.1 Administratively Controlled Information

Administratively Controlled Information is official information or material of a sensitive but unclassified nature, which does not contain national security information (and therefore cannot be classified). Nonetheless, ACI must be protected against inappropriate disclosure. Within NASA, such information may have previously been designated "FOR OFFICIAL USE ONLY." This NASA designation has been changed to "Administratively Controlled Information" for clarity and to more accurately describe the status of information to be protected.

2.2 Protecting Login Information

Work Group accounts are established in a manner that ensures access is granted on a need to know and least privilege basis. Work Groups rely on a combination of user name, which establishes the identity of the user for the computer or system, and a password, which is known only to the authorized user and authenticates that the user is who he or she claims to be. Passwords are simpler and cheaper than other, more secure forms of authentication such as special key cards, fingerprint ID machines, and retinal scanners. However, since they are a simpler and cheaper means of protecting a system or account, they require greater protection by the user. This includes the following:

- Passwords must be a minimum of eight characters. The eight characters will contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, and special characters.
- Never record login information in an unprotected location - electronic or physical, where unauthorized individuals can access it.
- If your Work Group will store ACI data, never transmit the user name or password by e-mail, fax, instant messaging, pager, or other electronic means. *The user name and password will always be provided verbally, once the user's secret question has been correctly answered for Work Groups that handle ACI data.*

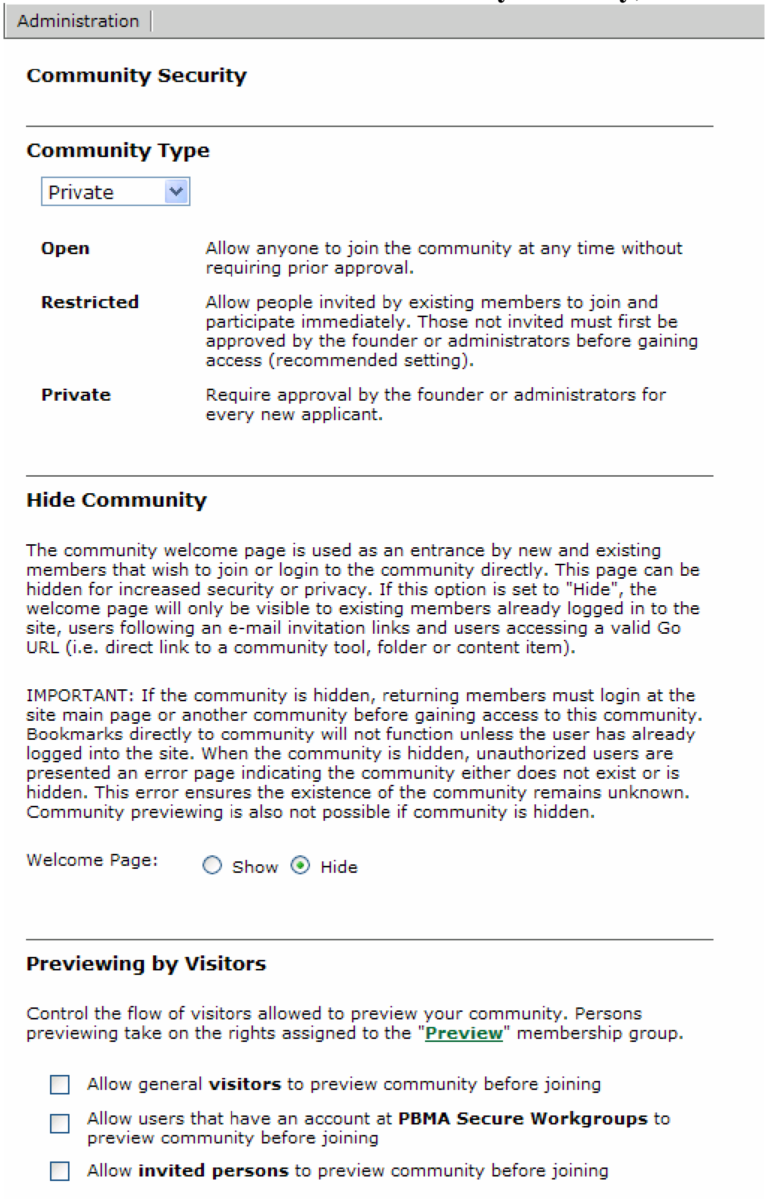
2.3 Work Group Configuration

Certain functions have been disabled in the application in order to support security standards. They include:

- “Remember Me” Functionality
- Automated Password Recovery

There are different membership roles within the application that hosts the Work Groups. The Work Group Founder (“Founder”) is the top-level role who approves any data that will reside in the Work Group and has complete control over all content and Work Group administration. The Originator is often, but not always, the Founder. This status also permits modification of Work Group specific security settings. It is imperative that the Founder take extreme care in enforcing baseline security requirements.

- Under **Administration → Community Security**, seen in



Community Security

Community Type

Private

Open Allow anyone to join the community at any time without requiring prior approval.

Restricted Allow people invited by existing members to join and participate immediately. Those not invited must first be approved by the founder or administrators before gaining access (recommended setting).

Private Require approval by the founder or administrators for every new applicant.

Hide Community

The community welcome page is used as an entrance by new and existing members that wish to join or login to the community directly. This page can be hidden for increased security or privacy. If this option is set to "Hide", the welcome page will only be visible to existing members already logged in to the site, users following an e-mail invitation links and users accessing a valid Go URL (i.e. direct link to a community tool, folder or content item).

IMPORTANT: If the community is hidden, returning members must login at the site main page or another community before gaining access to this community. Bookmarks directly to community will not function unless the user has already logged into the site. When the community is hidden, unauthorized users are presented an error page indicating the community either does not exist or is hidden. This error ensures the existence of the community remains unknown. Community previewing is also not possible if community is hidden.

Welcome Page: ○ Show ● Hide

Previewing by Visitors

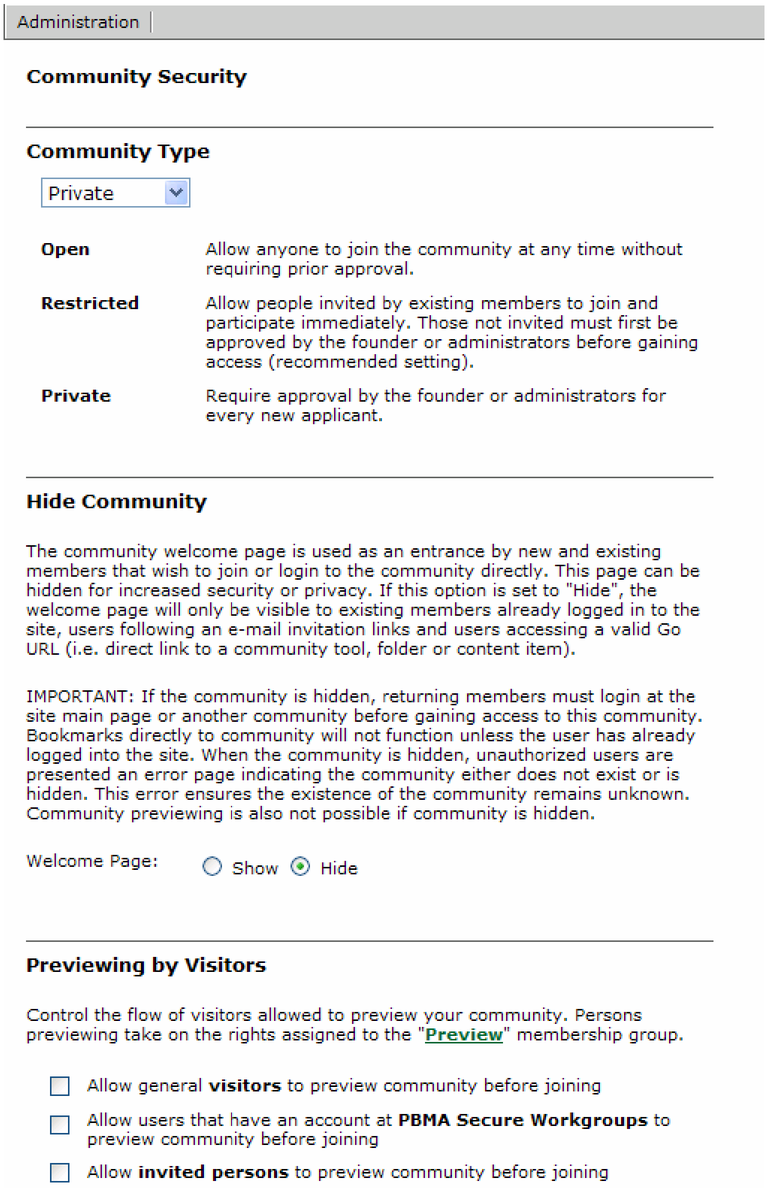
Control the flow of visitors allowed to preview your community. Persons previewing take on the rights assigned to the "Preview" membership group.

□ Allow general **visitors** to preview community before joining

□ Allow users that have an account at **PBMA Secure Workgroups** to preview community before joining

□ Allow **invited persons** to preview community before joining

Figure 1, these settings must not be altered if the Work Group stores ACI data. Altering these settings could allow unauthorized access.



Community Security

Community Type

Private

Open Allow anyone to join the community at any time without requiring prior approval.

Restricted Allow people invited by existing members to join and participate immediately. Those not invited must first be approved by the founder or administrators before gaining access (recommended setting).

Private Require approval by the founder or administrators for every new applicant.

Hide Community

The community welcome page is used as an entrance by new and existing members that wish to join or login to the community directly. This page can be hidden for increased security or privacy. If this option is set to "Hide", the welcome page will only be visible to existing members already logged in to the site, users following an e-mail invitation links and users accessing a valid Go URL (i.e. direct link to a community tool, folder or content item).

IMPORTANT: If the community is hidden, returning members must login at the site main page or another community before gaining access to this community. Bookmarks directly to community will not function unless the user has already logged into the site. When the community is hidden, unauthorized users are presented an error page indicating the community either does not exist or is hidden. This error ensures the existence of the community remains unknown. Community previewing is also not possible if community is hidden.

Welcome Page: ○ Show ● Hide

Previewing by Visitors

Control the flow of visitors allowed to preview your community. Persons previewing take on the rights assigned to the "Preview" membership group.

□ Allow general **visitors** to preview community before joining

□ Allow users that have an account at **PBMA Secure Workgroups** to preview community before joining

□ Allow **invited persons** to preview community before joining

Figure 1- The Community Security Screen

- Work Groups that contain ACI data shall always be “Private,” i.e., new Members must be invited and approved by the Founder or an Administrator in order to join the group. The Originator must maintain complete control of membership functions in Work Groups containing ACI data. (See Section 2.4.2 for further information on what constitutes ACI data.)
- All Work Groups will be set to “Private” by default.
- Work Groups that do not house ACI data may be set to “Open”.

2.4 Work Group Monitoring

2.4.1 Access Control

Originators are responsible for ensuring that membership is limited to individuals with a legitimate need to access their Work Group. Final membership authority will always reside with the Originator. Good security practices when monitoring membership in the Work Group include:

- Verifying who is requesting membership and their need for such membership. It is recommended that Originators of Work Groups containing ACI data make all End-users complete the National Agency Check form found in Appendix B – National Agency Check Verification (Appendix B).
- Removing Inactive Users. Note that if the End-user to be removed has been designated as an Administrator, Technical Support must be notified to complete the removal process.
- Deleting End-users who no longer require or are no longer involved in the process or activity supported by the Work Group.
- Deleting the entire Work Group or request site deactivation at conclusion of Work Group activity.
- Never accessing ACI data from a user's home computer.

2.4.2 Information

The Originator should review material in each of their Work Groups for possible designation as ACI prior to use. Criteria of at least one of the following must be met to qualify as ACI, as outlined in NPR 1600.1, *NASA Security Program Procedural Requirements,* Chapter 5.22:

- Information Protected by Statute: Export Administration Act; Arms Export Control Act; Space Act (Section 303b):
  - ITAR: International Traffic in Arms Regulations
  - EAR: Export Administration Regulations
  - MCTL: Military Critical Technologies List
  - FAR: Federal Acquisition Regulations
  - FOIA: Freedom of Information Act and the Privacy Act of 1996
  - UCNI: Unclassified Controlled Nuclear Information.
- Information the data owner determines to be unusually sensitive or critical to the success of the program or project.
- Information Exempt from Freedom of Information Act (FOIA); which includes:
  - Internal Personnel Rules/Practices
  - Trade Secrets/Commercial/Financial
  - Inter/Intra-Agency Memos and Letters
  - Personnel and Medical Files
  - Investigative Records
  - Financial Institution Information
  - Geological/Geophysical

- Maps/Documents of underground utilities
- Drawings/specifications for Mission Essential Infrastructure (MEI) or other assets
- Mission specific security plans
- Emergency Contingency plans

3 PROCESS FOR ACTIVATING A NEW WORK GROUP

The process for activating a new Enhanced Security Work Group is displayed below in The Work Group Activation Process Swim Lane Diagram. The set of tasks that the Originator must perform are located in the topmost swim lane labeled 'Work Group Originator'. These tasks are discussed in the sections following the figure.

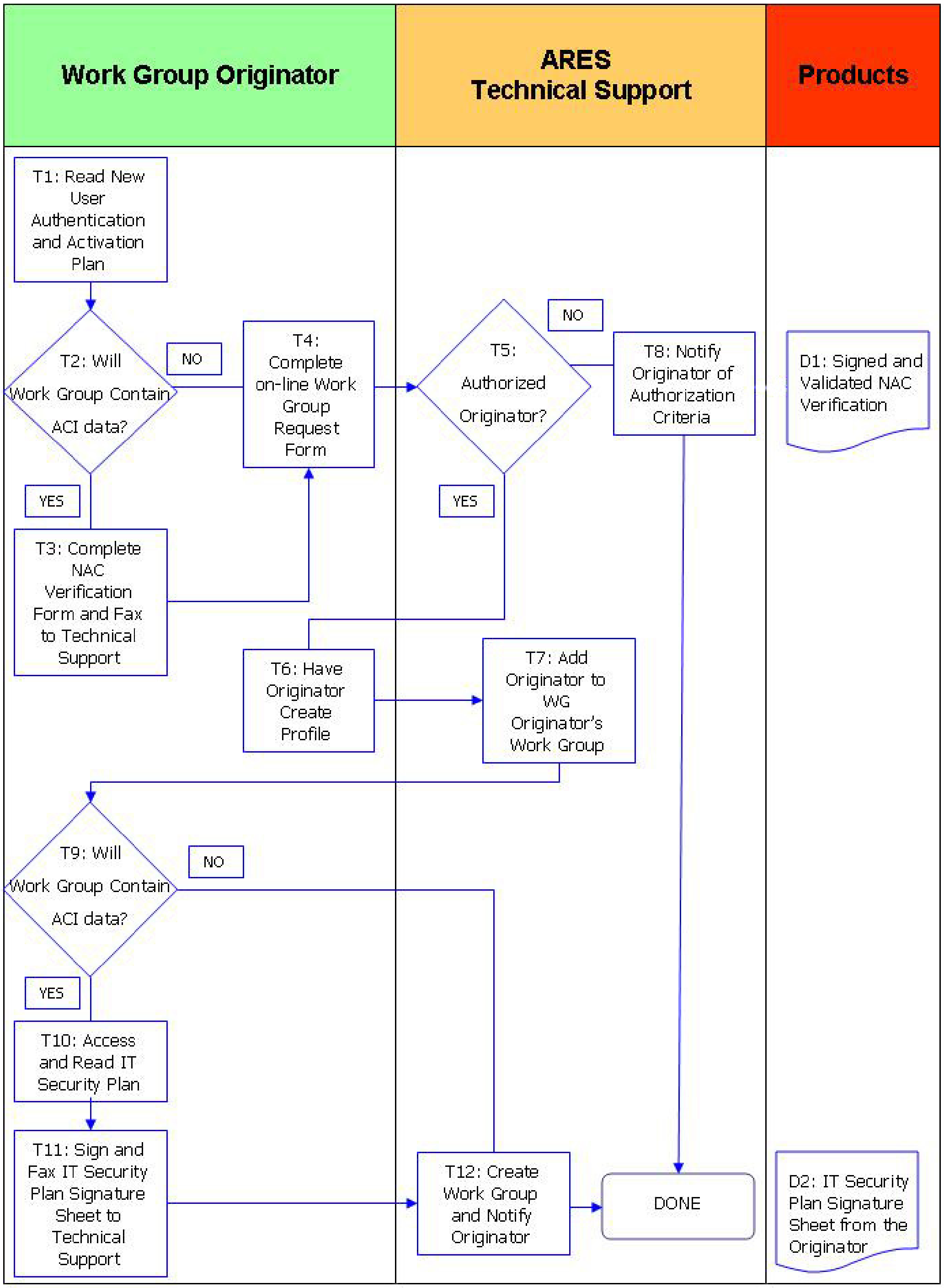

Work Group Originator
ARES Technical Support
Products
T1: Read New User Authentication and Activation Plan
T2: Will Work Group Contain ACI data?
NO
YES
T3: Complete NAC Verification Form and Fax to Technical Support
T4: Complete on-line Work Group Request Form
T5: Authorized Originator?
NO
YES
T8: Notify Originator of Authorization Criteria
D1: Signed and Validated NAC Verification
T6: Have Originator Create Profile
T7: Add Originator to WG Originator's Work Group
T9: Will Work Group Contain ACI data?
NO
YES
T10: Access and Read IT Security Plan
T11: Sign and Fax IT Security Plan Signature Sheet to Technical Support
T12: Create Work Group and Notify Originator
DONE
D2: IT Security Plan Signature Sheet from the Originator

Figure 2: The Work Group Activation Process Swim Lane Diagram

3.1 Read Enhanced Security Work Group NUAAP

STEP T1: The Originator must begin by reading the NUAAP (this document), which contains the ESWG General Charter located in Appendix A – PBMA Enhanced Security Work Groups Charter (Appendix A), the basic procedures to activate a Work Group, and the necessary security practices. The purpose of reading the NUAPP is for the Originator to become familiar with the purpose and responsibilities associated with running a new Work Group.

⇒ The PBMA Program Management reserves the right to deny requests for activation of any Work Group or to delete any existing Work Group that does not comply with the intent of the Enhanced Security Work Groups General Charter.

3.2 Determine Data Content

STEP T2: The Originator must determine if the Work Group will contain ACI data prior to submitting the request to create the Group. Please see 2.4.2 of this document or NPR 1600.1, *NASA Security Program Procedural Requirements*, Chapter 5.22, which lists the criteria for determining ACI data. If the Work Group will contain ACI data, continue to Complete the NAC Verification Form. If not, continue to 3.4 instead.

3.3 Complete the NAC Verification Form

STEP T3: If the Work Group *will* contain ACI data, the Originator must fill out the National Agency Check Verification form located in Appendix B of this document. The Originator is also responsible for verifying their End-user's ability to access ACI data.

Once completed, the Originator will fax the completed NAC verification form to Technical Support at 440-962-3098.

3.4 Complete Online Work Group Request Form

STEP T4: The Originator can now request a new Enhanced Security Work Group through the PBMA-KMS Web site at http://pbma.nasa.gov/secureworkgroups_main_cid_19. To make this request, perform the following steps:

1. Select a Work Group name.
2. Click the *Request a New Enhanced Security Work Group* tab on the left-hand navigation bar to access the on-line request form.
3. Once you have filled in the required information, click the *Send* button to send the form to Technical Support.

   ⇒ Once a new Work Group request has been granted, the group's Founder or Administrator shall be responsible for the customization of Work Group settings, approval of individuals for membership, and uploading of all default content.

3.5 Create New Profile for Originator

STEP T6: Once the Originator has met the criteria for obtaining a Work Group, Technical Support will send notification to the Originator to create their account. To create this account, perform the following steps:

1. Go to https://secureworkgroups.grc.nasa.gov.
2. Click the "Create an account" link.
3. Fill out the on-line form and click the "Create Account" button to complete the process.

Once the Originator's account is created, it will then be added to the Originator's Work Group. This Work Group has been created for information that pertains specifically to Originators.

3.6 Approvals Required for ACI Capable Work Groups

STEP T9: The Originator must determine if the Work Group will handle ACI data. Each Originator is also responsible for verifying their End-user's ability to access ACI data as per Code I requirements.

Work Groups are available to all NASA and contractor personnel, industry partners and academia. All Originators are required to submit proof of United States citizenship via the National Agency Check Verification form found in Appendix B – National Agency Check Verification (Appendix B).

It is strongly recommended that Originators of Work Groups containing ACI data make *all* End-users complete the National Agency Check Verification form.

3.7 Access the PBMA ESWG IT Security Plan

STEP T10: Once an Originator's request for an ACI-capable Work Group is approved and the Originator has created their account, they will be added to the requested Work Group. They will also be added to the "ACI Originators" user-group. This allows them to access the *PBMA ESWG IT Security Plan* ("IT Security Plan").

⇒ Users of the Enhanced Security Work Groups will only have one account. One user ID and one password will be used for access to all Enhanced Security Work Groups that the user has membership in.

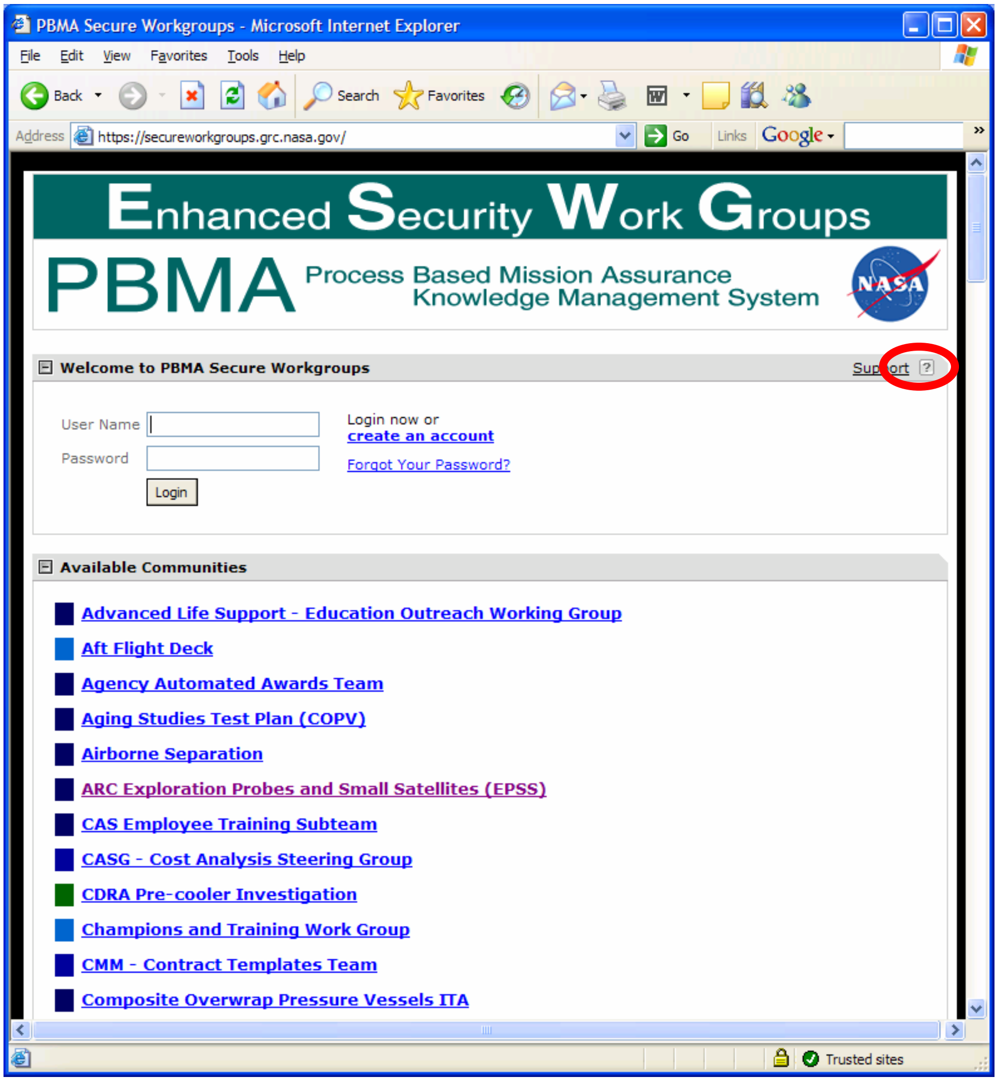
3.8 Sign PBMA ESWG IT Security Plan

STEP T11: Once the Originator accesses and reads the IT Security Plan, they must sign the plan's signature sheet. By signing, the Originator gives consent as the Data Owner for the sensitive information to reside on the Work Group. The signature sheet, with the Originator's original signature, must be faxed to Technical Support at 440-962-3098.

⇒ The Work Group cannot be activated without the Originator's signature on the *PBMA ESWG IT Security Plan*.

4 GETTING HELP

You can call up the **Help** window by clicking the **?** link on the **Login** webpage as seen in Figure 3.


PBMA Secure Workgroups - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
https://secureworkgroups.grc.nasa.gov/
Go
Links
Google
Enhanced Security Work Groups
PBMA
Process Based Mission Assurance
Knowledge Management System
NASA
Trusted sites

Welcome to PBMA Secure Workgroups
Support ?

User Name
Password
Login

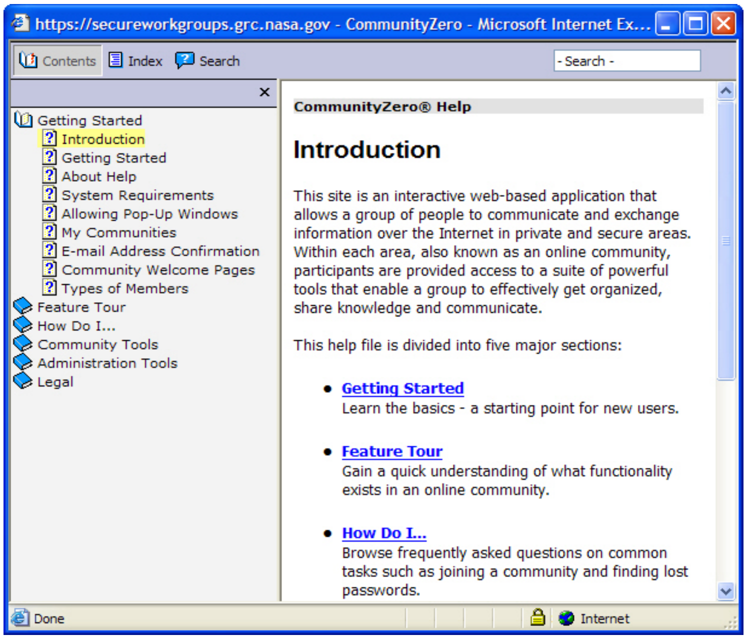
Login now or
create an account
Forgot Your Password?

Available Communities

- Advanced Life Support - Education Outreach Working Group
- Aft Flight Deck
- Agency Automated Awards Team
- Aging Studies Test Plan (COPV)
- Airborne Separation
- ARC Exploration Probes and Small Satellites (EPSS)
- CAS Employee Training Subteam
- CASG - Cost Analysis Steering Group
- CDRA Pre-cooler Investigation
- Champions and Training Work Group
- CMM - Contract Templates Team
- Composite Overwrap Pressure Vessels ITA

Figure 3: The Enhanced Security Work Groups Login webpage

The **Help** window is displayed as seen in The Help Window. You can either use the application's search engine to look for the answer to a question, or you can look it up in the applications contents, listed on the left hand side of the window.



CommunityZero® Help

Introduction

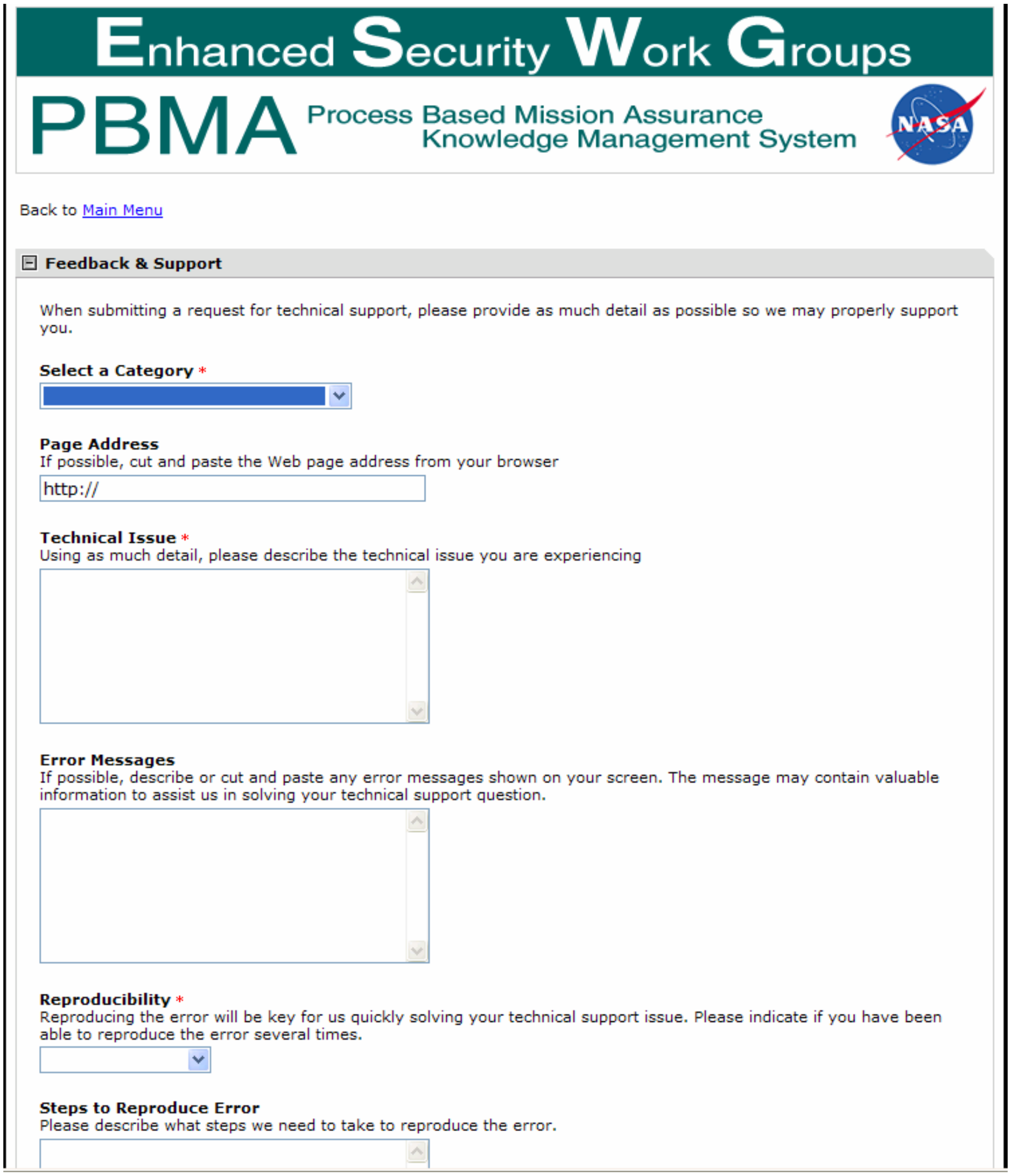
This site is an interactive web-based application that allows a group of people to communicate and exchange information over the Internet in private and secure areas. Within each area, also known as an online community, participants are provided access to a suite of powerful tools that enable a group to effectively get organized, share knowledge and communicate.

This help file is divided into five major sections:

- **Getting Started**
  Learn the basics - a starting point for new users.
- **Feature Tour**
  Gain a quick understanding of what functionality exists in an online community.
- **How Do I...**
  Browse frequently asked questions on common tasks such as joining a community and finding lost passwords.

Figure 4: The Help Window

Technical support is also available when the information provided in this document and online **Help Window** proves insufficient. All support issues will be routed to the Help Desk via the *Support* link on the **Login** webpage, located next to the ***?*** link. Clicking the *Support* link will bring up the initial **Feedback & Support** page seen below in Figure 5.


Enhanced Security Work Groups
PBMA Process Based Mission Assurance
Knowledge Management System
NASA

Back to Main Menu

⊟ Feedback & Support

When submitting a request for technical support, please provide as much detail as possible so we may properly support you.

Select a Category *

Page Address
If possible, cut and paste the Web page address from your browser

http://

Technical Issue *
Using as much detail, please describe the technical issue you are experiencing

Error Messages
If possible, describe or cut and paste any error messages shown on your screen. The message may contain valuable information to assist us in solving your technical support question.

Reproducibility *
Reproducing the error will be key for us quickly solving your technical support issue. Please indicate if you have been able to reproduce the error several times.

Steps to Reproduce Error
Please describe what steps we need to take to reproduce the error.

Figure 5: The Feedback & Support webpage

Technical Support can be contacted via the **Feedback & Support** webpage or by sending a detailed email to the following address:

pbma_workgroup@arescorporation.com

All requests will be handled as quickly as possible. Any requests received outside of standard operating hours will be resolved as soon as possible the following business day.

APPENDIX A – PBMA ENHANCED SECURITY WORK GROUPS CHARTER

NASA Process Based Mission Assurance Enhanced Security Work Groups (PBMA ESWG) General Charter

Enhanced Security Work Groups are available as an enhanced functionality of Process Based Mission Assurance (PBMA). These Enhanced Security Work Groups provide multi-dimensional, collaborative functionality to support the NASA Safety and Mission Assurance community, individual program/project teams as well as formal and informal groups of subject matter experts.

Enhanced Security Work Groups for Sensitive Data

Membership is limited to those individuals involved in making NASA programs and projects successful, including contractors, industry partners, and academia. Membership in the community is predicated on the notion of reciprocity and sharing of knowledge as well as responsiveness to the needs and inquiries of the community.

Legal/Security Ground Rules

- No classified information.
- Work Group Members must be verified by their Work Group Originator.

Enhanced Security Work Groups for Non-Sensitive Data

Enhanced Security Work Groups are available for those groups that do not have a need to handle sensitive information. These Work Groups **DO NOT** have authorization to share ITAR/EAR, SEB or other sensitive information that falls under the classification of ACI.

These Work Groups have the same functionality as those that handle ACI and can be used for that purpose once the Work Group Originator has completed the process (http://pbma.hq.nasa.gov/swg/activation_process.htm) of signing the *PBMA ESWG IT Security Plan* and submitting the NAC Verification Form.

Legal/Security Ground Rules

- No classified information.
- No material protected under Federal Export Control and International Traffic in Arms Regulations.
- No competition sensitive or proprietary information.
- No other sensitive material within the ACI category.

For additional information on these topics please contact your center Export Administrator or Export Counsel listed at:
http://www.hq.nasa.gov/office/codei/nasaecp/

Or access the following NASA documents:

- OMB Circular A-130
- NPR 2190.1: NASA Export Control Program
- NPD 2110.1: Foreign Access to NASA Technology Utilization Material
- NPD/NPG 2800.1: Managing Information Technology
- NPD/NPG 2810.1: Security of Information Technology
- NPR 1600.1: NASA Security Program Procedural Requirements
- NIST 800-53: Recommended Security Controls for Federal Information Systems

Work Group Originator Requirements

- Review information content of the community space to assure the Work Group is not violating NASA policies regarding information security and technology transfer
- Manage and control Work Group membership and access
- Notify new members that join the Work Group outlining their responsibilities
- Prepare concise Work Group statement of purpose (two or three sentences)
- Prepare Work Group charter (two or three paragraphs)
- Visit community space on a regular basis and add new information, update or remove old information
- Mentor new members in the general functioning of the specific community

Work Group Member Requirements

- Activities that will not be tolerated and are grounds for termination of participation include:
    - Using the community space for unprofessional means, i.e., spamming, flaming, etc.
    - Violating the NASA policies regarding information disclosure
    - Violating the NASA policies regarding security and personnel safety
- Review the community-specific charter and pertinent literature including postings to the community space
- Biographical sketch for posting in the community space

Work Group Support Activity

- Periodic workshops will be conducted providing lessons learned and best practice case studies for Work Group Originators
- General metrics such as number of members, last date of activity within a Work Group, etc., will be collected and reported to PBMA management

APPENDIX B – NATIONAL AGENCY CHECK VERIFICATION

NAC Verification Form for PBMA Enhanced Security Work Groups

All Enhanced Security Work Groups that contain ACI data require that you must have the approval signature of your appropriate Center's security personnel. Requests should be delivered to PBMA ESWG Technical Support, c/o ARES Corporation, 21000 Brook Park Rd., MS 501-4, Cleveland, OH 44135, or

Fax completed form to 440-962-3098.

Name ______________________________ Title ______________________________

Center ______________________________ Work Phone ________________________

Organization _________________________ E-mail Address _____________________

You are requesting access to a Secure Work Group that will be approved for sensitive but unclassified data.

You agree that unauthorized use of the computer accounts and computer resources to which you are granted access may be a violation of NPG 2810.1 and NPR 2190.1. You will make every effort to protect your account(s) from unauthorized access and will not knowingly permit access by others. Misuse of your assigned account and by accessing others' accounts without authorization is not allowed. You understand that these resources are subject to monitoring and recording by the Glenn Research Center to detect unauthorized use in accordance with NPG 2810.1. You further understand that failure to abide by these provisions may constitute grounds for termination of account access, administrative action, and/or civil or criminal liability as set forth in NPG 2810.1, NPR 2190.1, NPR 1600.1 and other applicable laws and regulations.

All users must follow these additional rules:

- NO Classified Information may be posted in these Work Groups
- Protect data as outlined in Section 2 of the PBMA ESWG New User Authentication And Activation Plan (NUAAP)
- Enhanced Security Work Groups are to be used for official NASA business ONLY

I certify that I am a United States citizen and have had a National Agency Check (NAC) performed.

I, ____ hereby certify that I understand, and upon the granting of access to the Web server shall comply with all above statements.

____ ____________________
Work Group Originator Signature Date

_________________________ ____________________ ____________________
Center Security Representative Signature Phone Number Date

For Internal Use Only

____ ____________________
Verification of Citizenship and NAC by Technical Support **Date**